WRITTEN STATEMENT
OF
MAUREEN COONEY
ACTING CHIEF PRIVACY OFFICER
CHIEF FREEDOM OF INFORMATION ACT OFFICER
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE HOUSE HOMELAND SECURITY
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING,
AND TERRORISM RISK ASSESSMENT
U.S. HOUSE OF REPRESENTATIVES

April 6, 2006

Introduction

Chairman Simmons, Ranking Member Lofgren, and Members of the Subcommittee, it is an honor to testify before you today on privacy activities at the United States Department of Homeland Security, with particular reference to privacy as part of the Department's Intelligence Enterprise.

Because this marks my first appearance before the Subcommittee, I would like to offer some biographical background. It is my honor to currently serve as the Acting Chief Privacy Officer for the Department of Homeland Security. I come to this post with 20 years of federal experience in risk management and compliance and enforcement activities as well as in consumer protection work on global information privacy and security issues post 9-11. I was recruited from the Federal Trade Commission to join the Department of Homeland Security more than two years ago as Chief of Staff of the Privacy Office and Senior Advisor for International Privacy Policy. Since that time, it has been my privilege to help build the DHS Privacy Office, under the leadership of former Chief Privacy Officer, Nuala O'Connor Kelly, and Secretaries Chertoff and Ridge.

As the Subcommittee well knows, the Department of Homeland Security was the first agency to have a statutorily required Privacy Officer. The inclusion of a senior official accountable for privacy policy and protections within the Department honors the value placed on privacy as an underpinning of our American freedoms and democracy. It also reflects Congress' understanding of the growing sensitivity and awareness of the ubiquitous nature of personal data flows in the private and public sectors and a recognition of the impact of those flows upon our citizens' lives.

In addressing the Department's Data Privacy and Integrity Advisory Committee, which was created to advise the Secretary and the Chief Privacy Officer on significant privacy issues, Secretary Michael Chertoff recently noted that the Department has the opportunity to build into the "sinews of this … organization, respect for privacy and a thoughtful approach to privacy." Secretary Chertoff expressed a belief that I share:

We want the government to be a protector of privacy, and we want to build security regimes that maximize privacy protection and that do it in a thoughtful and intelligent way . . . . [I]f it's done right,[it] will be not only a long-lasting ingredient of what we do in Homeland Security, but a very good template for what government ought to do in general when it comes to protecting people's personal autonomy and privacy.[1]

The Chief Privacy Officer[2] and the DHS Privacy Office have a special role, working in partnership and collaboration across the Department, to integrate privacy into the consideration of the ways in which the Department assesses its programs and uses technologies, handles information, and carries out our protective mission. The Privacy Office has oversight of privacy policy matters and information disclosure policy, including compliance with the *Privacy Act of 1974*, the *Freedom of Information Act*, and the completion of Privacy Impact Assessments on all new programs, as required by the *E-Government Act of 2002* and Section 222 of the *Homeland Security Act of 2002*. The Privacy Office also evaluates new technologies used by the Department for their impact on personal privacy. Further, under Section 222, the Chief Privacy Officer is required to report to Congress on these matters, as well as on complaints about possible privacy violations.

Today, I would like to describe for you how the Privacy Office has worked to build privacy into the sinews of our organization so that a culture of privacy informs the way in which we carry out our national mission of protecting our homeland. I'll explain our operational approach of embedding adherence to good privacy practices into the programs of the Department, through the budget and design phases of programs, through accountability and transparency tools, including reviews of privacy notices (systems of

---

[1] March 7, 2006 public Meeting of the Department of Homeland Security Data Privacy and Integrity Advisory Committee, Ronald Reagan Building and International Trade Center, Washington, D.C.

[2] The DHS Chief Privacy Officer is the first statutorily required privacy officer in the federal government. Section 222 of the Homeland Security Act, as amended, provides in pertinent part, the responsibilities of the DHS Chief Privacy Officer are to assume primary responsibility for privacy policy, including –

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection and disclosure of personal information;

(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and

(5) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls and other matters.

records notices), the use of privacy impact assessments, and privacy audits and reviews. Our approach is consistent for all DHS programs and initiatives and we have found that it works equally well for the law enforcement, homeland security and intelligence functions of the Department.

I would then like to focus on the mandates of information sharing and intelligence activities and how those imperatives for national preparedness can be achieved while integrating privacy attentiveness and protections into Departmental operations.

Building a Culture of Privacy

The Privacy Office works in partnership with each DHS Directorate and component to promote a business ethic of privacy attentiveness and responsible stewardship for the personal information that we collect, use and disseminate. This is fundamental to the Department's overall achievement of its mission and for engendering the trust of the American people and visitors to our nation.

We operationalize privacy at the outset of DHS program initiation through two primary means. First, the Privacy Office works to incorporate privacy in the development processes used to build DHS information systems. Second, the Privacy Office confirms that privacy is embedded in the information systems that involve personal data through the privacy assessment process. These two methods allow the Privacy Office to "bake" privacy into Departmental operations.

Building privacy into the development process starts with the investment review processes for major programs and information systems at the Department. In partnership with the DHS Management Directorate, the Privacy Office participates on three separate committees that review project proposals and set performance criteria for program and technology investment budget approvals. We thus can use the "power of the purse" to ensure that program personnel are attentive to privacy requirements.

The Privacy Office then works to operationalize privacy protections through "privacy gateways" that focus on the projected design and use of an information technology system. In collaboration with the Office of the Chief Information Officer, the Privacy Office is developing these "privacy gateways" for the systems development life cycle review of technology deployed for Departmental programs to ensure that privacy practices are integrated through a monitored and auditable process.

Consequently, Department design and deployment initiatives move forward only after proper attention has been paid not only to operational issues, but also to privacy issues. In fact, privacy is considered a cornerstone of the Department's program architecture, consistent with the mandate to protect the homeland while preserving essential liberties.

Once funding for an information system is determined and privacy is considered in the systems development life cycle, the Privacy Office monitors privacy compliance through the use of a Privacy Impact Assessment (PIA). Conducting PIAs demonstrates the Department's efforts to assess the privacy impact of utilizing new or significantly changing information systems, including attention to mitigating privacy risks. Touching

on the breadth of privacy issues, PIAs allow the examination of the privacy questions that may surround a program or system's collection of information, as well as, the system's overall development and deployment.

When worked on early in the development process, PIAs provide an opportunity for program managers and system owners to build privacy protections into a program or system in the beginning. This avoids forcing the protections in at the end of the developmental cycle when remedies can be more difficult and costly to implement. In accordance with Section 208 of the *E-Government Act of 2002* and OMB's implementing guidance, the Department of Homeland Security is required to perform PIAs whenever it procures new information technology systems or substantially modifies existing systems that contain personal information. The Chief Privacy Officer reviews and signs off on all Departmental PIAs and then they are published.

Although the *E-Government Act* allows exceptions from the PIA requirement for national security systems, as a matter of good privacy practice, the Privacy Office requires that *all* DHS systems, including national security systems, undergo a PIA if they contain personal information. We use the PIA process as a good government information management tool and privacy protective process across the Department's programs. In cases where the publication of the PIA would be detrimental to national security, the PIA document may not be published or may be published in redacted form. This means that information systems that are part of the Intelligence Enterprise at the Department undertake these important analyses to ensure that privacy considerations are fully integrated. Our intelligence information systems are better considered and developed as a result of conducting PIAs.

Transparency and Accountability

To assure that information in DHS record systems is handled in a manner consistent with the fair information practices principles set out in the *Privacy Act of 1974*, the Privacy Office carefully reviews new Systems of Records Notices and new initiatives that seek to collect information to be placed under existing SORNs. The Privacy Office works closely with the Office of the General Counsel on the legal issues attendant to these SORNs and with all DHS program offices to analyze the ways in which the information will be shared through approved routine uses. In addition to SORNs, we benchmark programs' compliance with fair information practices principles based upon their development and adherence to internal policies, procedures, and public statements of program goals. To that end, we are working on a privacy tool that will assist programs in doing periodic self assessments against similar measures.

Another way the Privacy Office encourages transparency and accountability is through outreach and public workshops. Just yesterday, the Privacy Office hosted a public event concerning *Transparency and Accountability: The Use of Personal Information within the Government.* We explored the front end of the privacy process – how public notices inform the public of the intended use of personal information by government – and the back end of the process – how government can live up to the promises made in public notices through mechanisms for appropriate access, including

through *Privacy Act* disclosures, *Freedom of Information Act* disclosures, and other appropriate means.

Privacy Audits and Reviews

The Privacy Office also has an important oversight function within the Department in assessing whether the fair information practices embedded in the *Privacy Act of 1974* are appropriately implemented in our programs, along with other relevant frameworks. We do this through privacy audits and providing guidance at points along the development of programs. While the Privacy Office has an important internal role, it also receives and reports on complaints and concerns from the public about the privacy attentiveness of DHS programs. In response, we undertake reviews of those concerns and report on them to the Secretary and to Congress, per Section 222 of the *Homeland Security Act*, providing constructive guidance.

Privacy Protection and Public Security through Information Sharing and Intelligence

The Department of Homeland Security was created, in significant part, to foster information sharing for homeland security purposes. And from its beginning, the Department has undertaken the important work of removing the invisible barriers that block appropriate information flows within the Department. The *Privacy Act*, of course, provides the statutory authority for intra-agency information sharing when there is a need to know, and Privacy Office policy supports the exchange of information between the Department's component organizations whenever the organizations establish an appropriate need based on an express purpose. The Privacy Office, therefore, works with Department components to facilitate the exchange of information in a privacy sensitive manner, while working toward the goal of the right persons getting the right information at the right time.

The Department must also foster external information sharing for homeland security purposes with all of our partners at the Federal, state, local, tribal and private sector levels. As the Department incorporates the "need to share," in its information sharing design it is, of course, paramount that privacy be built into the process. Our work on internal information sharing complements and informs the Department and Privacy Office's efforts to assist with external information sharing efforts.

Just as the sharing model has changed, so must the paradigm shift to enhanced, stronger, and embedded privacy protections because, as Secretary Chertoff has said, "When we share information, if we do it in a disciplined way, we actually elevate the security of both those who share - and those who receive - the information." The Privacy Office has therefore worked diligently to help create an information sharing model that allows for robust information exchanges for homeland security purposes even while it fosters robust privacy protections.

In particular, we have worked collaboratively with our Intelligence and Analysis colleagues, for whom information sharing is part of their critical mission, to ensure that personally identifiable information of U.S. persons is treated in a manner that fully conforms with their rights and is handled sensitively. The DHS policy on handling U.S.

person information developed by the Intelligence and Analysis section of DHS contains a significant role for the DHS Privacy Officer to review activities that could involve a potential violation of the privacy rights of U.S. citizens and also requires the Privacy Officer to collaborate on new initiatives to ensure that they enhance and do not erode privacy protections relating to the collection, use and maintenance of personal information. This policy is another example of the way that the Privacy Office has helped to construct a culture of privacy at DHS and has worked to make privacy an operational imperative as we move forward with our mission.

Related to these activities is the fact that over the past four years, the Administration has provided new tools to permit federal agencies to exchange information. Most recently, in Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, which was issued on October 25, 2005, the President made clear his intent that all federal agencies work to prepare an environment in which information flows support counterterrorism functions. The Executive Order specifically recognizes the importance of protecting the "freedom, information privacy, and other legal rights of Americans." This message is further reflected in the *Presidential Memorandum* of December 16, 2005, to all federal departments and agencies providing guidelines and specific requirements to build the new Information Sharing Environment.

As part of this Memorandum, the President issued Guideline 5 stating that "the Federal Government has a solemn obligation, and must continue fully, to protect … the information privacy rights and other legal rights of Americans…" in the building of an information sharing environment.

In parallel with the President's efforts, Congress enacted three laws providing the U.S. Government with greater authority for collecting, analyzing, and disseminating terrorist information: the *USA PATRIOT Act of 2001*, the *Homeland Security Act of 2002*, and the Intelligence *Reform and Terrorism Prevention Act of 2004* (IRTPA). This last statute puts in place a mechanism to formalize the creation of the information sharing environment on an interagency level and it, too, provides that the privacy rights of individuals must be central to the environment's creation.

"Need to Share" and the Role of the DHS Privacy Office

Recent legislative enactments confirm what the National Commission on Terrorist Attacks Upon the United States recommended and that the President has required in his Executive Orders on information sharing, that we have moved from a "need to know" environment to a "need to share" environment. This "need to share" presents significant improvements to information exchange, but it also presents significant challenges to individual expectations for privacy and to institutional privacy safeguards. At the Department of Homeland Security, as we move forward in our ability to share data, we are aware of our responsibility for the privacy, security and authorized use of the data entrusted to us.

Specifically, technology and information policy should be maximized to build privacy protections into data sharing models. But technology and privacy awareness, while important tools in protecting individual privacy interests, will not be enough to

address current challenges. As we move forward, we will also need to establish and enforce concrete safeguards to prevent unauthorized access, use, or disclosure.

The Privacy Office has provided expertise and guidance for building the ISE by working closely with the Information Sharing Environment Program Manager (ISE/PM) and various steering groups on issues not only dealing directly with privacy, but also with subjects such as governance, operations, and harmonization of technologies. Through these efforts, the Privacy Office is assisting with facilitating the incorporation of privacy protections at the roots of the ISE development.

Currently, the Privacy Office is a member of an interagency working group, operating under the joint leadership of the Director of National Intelligence and the Department of Justice, as specified by the President under Guideline 5. This group will conduct a review of current executive department and agency information sharing policies and procedures regarding the protection of information privacy and other legal rights of Americans; and develop guidelines designed to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including in the acquisition, access, use, and storage of personally identifiable information.

The review of policies is focusing on coordinating and consolidating the work already done to focus on the key issues to harmonizing privacy protections. This review will lead into the development of appropriate guidelines that will outline a process for the operation of the entire ISE.

Conclusion

The Privacy Office will continue to work to ensure that privacy is woven into the very fabric of the Department as a guiding principle and value through operationalizing privacy throughout the Department and responding to privacy concerns about information sharing environments in positive, constructive ways.

In addition, as the Acting Chief Privacy Officer of DHS, I endeavor at all times to keep an open door to the privacy community around the nation and the world to ensure that the Department benefits from the range and depth of privacy practitioners and concerned citizens everywhere.

We face great challenges. But we must achieve both security and privacy and, with both, sustain our values and freedoms. I do not doubt that we can move forward together and achieve our mission of protecting and preserving our lives and our way of life, preserving our Liberty and with it, our privacy. I appreciate the opportunity to testify before this important committee today. I look forward to hearing the other witnesses' testimony and to answering your questions.